COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 43, No. 1 1994

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171 JAPAN

A Construction of Algebraic Curves Whose Jacobians Have Non-trivial Endomorphisms

by

Ichiro SHIMADA

(Received September 16, 1993; revised February 1, 1994)

Introduction

In this paper, we study certain correspondences of an algebraic curve which arises naturally from a non-Galois branched covering over the projective line, and construct algebraic curves such that the endomorphism rings of their jacobians contain the integer ring of a quadratic number field. Throughout this paper, we work over the complex number field $\mathbb{C}$.

An example of our construction is as follows. Let

$$U=\mathbb{P}^1\setminus\{P_1, \cdots, P_\mu, P_{\mu+1}, \cdots, P_{\mu+\nu}, \infty\} \qquad (\mu>0, \nu>0)$$

be a Zariski open subset of $\mathbb{P}^1$, with a base point $b\in U$. Then $\pi_1(U, b)$ is a free group generated by $\mu+\nu$ elements $[\alpha_1], \cdots, [\alpha_{\mu+\nu}]$. Let $l=2m+1$ be a prime number $\geqq 5$, and let $t\in\mathbb{F}_l^\times$ be a generator of the subgroup $\{x^2; x\in\mathbb{F}_l^\times\}$ of index 2 of $\mathbb{F}_l^\times$. Let $\mathfrak{S}(\mathbb{F}_l)$ denote the permutation group of the set $\mathbb{F}_l$. We give a group homomorphism $\phi: \pi_1(U, b)\to\mathfrak{S}(\mathbb{F}_l)$ by

$$x^{\phi([\alpha_i])}=\begin{cases} x+1, & \text{if } i=1, \cdots, \mu; \\ tx, & \text{if } i=\mu+1, \cdots, \mu+\nu, \end{cases}$$

for $x\in\mathbb{F}_l$. Then we can construct an étale covering $X\to U$ of degree l corresponding to ϕ. Let C be the compactification of X. Then the endomorphism ring of the jacobian variety of C contains the integer ring of the quadratic field $\mathbb{Q}(\sqrt{l^*})$ where $l^*=(-1)^{(l-1)/2}l$. We can also give an explicit description of the correspondence $D\to C\times C$ which induces the multiplication by $(-1+\sqrt{l^*})/2$ on the jacobian variety. Note that the covering $C\to\mathbb{P}^1$ is non-Galois.

In general, we can construct a correspondence $D\to C\times C$ from a non-Galois branched covering $C\to\mathbb{P}^1$ in the following way. Let $D\to C\to\mathbb{P}^1$ be the Galois closure of $C\to\mathbb{P}^1$ with the Galois group G, and let $H\subset G$ be the subgroup corresponding to $\pi: D\to C$. Since $C\to\mathbb{P}^1$ is non-Galois, H is not normal in G. Therefore, there is an element $g\in G$ such that $gHg^{-1}\neq H$. However the quotient $gHg^{-1}\setminus D$ is isomorphic to C, because their function fields are isomorphic over $\mathbb{C}$. The quotient map $D\to gHg^{-1}\setminus D$ gives another covering $\pi': D\to C$. From these π and π', we get the

correspondence $(\pi, \pi') : D \to C \times C$.

Of course, every algebraic curve admits a non-Galois branched covering over $\mathbb{P}^1$, while almost all jacobians have the trivial endomorphism ring $\mathbb{Z}$ (cf. [2]). Therefore, it is interesting to study when this kind of natural correspondences gives a non-trivial endomorphism of the (co-)homology group of the curve C. This is the main theme of this article. A partial answer to this question is given in §4. That is, the induced endomorphism is trivial (i.e., multiplication by an integer), if the Galois group G, considered as a subgroup of the permutation group of a general fiber of $C \to \mathbb{P}^1$, is 2-transitive. The detail of the above example is explained in §7.

The author would like to thank Prof. T. Shioda and Prof. T. Terasoma for helpful discussions and comments.

Conventions. Let I be the closed interval $[0, 1]$. Let $\alpha : I \to X$ and $\beta : I \to X$ be two paths such that $\alpha(1) = \beta(0)$. Then we denote the composition of these paths by $\alpha \cdot \beta$ or simply $\alpha\beta$. For a path α, we denote by $[\alpha]$ the homotopy equivalence class of paths with the fixed start and end points.

§1. Topological construction of the correspondences

Let $U \subset \mathbb{P}^1$ be a non-empty Zariski open subset of $\mathbb{P}^1$. We fix a base point $b \in U$. Let $(\tilde{U}, \tilde{b}) \to (U, b)$ be the universal covering. As a set, $\tilde{U}$ is the set of homotopy equivalence classes $[\alpha]$ of paths $\alpha : I \to U$ such that $\alpha(0) = b$. Then the natural projection $\tilde{U} \to U$ is given by $[\alpha] \mapsto \alpha(1)$. By the convention above, the fundamental group $\pi_1(U, b)$ acts on $\tilde{U}$ from left as deck transformations. Let $p : X \to U$ be an étale surjective morphism of degree k, where X is supposed to be connected. We put $B := p^{-1}(b) = \{b_1, \cdots, b_k\}$. For each $b_i \in B$, the natural homomorphism $\pi_1(X, b_i) \to \pi_1(U, b)$ is injective, whose image we shall denote by Γ_i. For a path $\alpha : I \to U$ such that $\alpha(0) = b$, we denote by $\alpha\langle X, b_i\rangle$ the lifting of α to X such that $\alpha\langle X, b_i\rangle(0) = b_i$. Using this notation, we have

$$\Gamma_i = \{[\gamma] \in \pi_1(U, b) ; \gamma\langle X, b_i\rangle(1) = b_i\} .$$

It is easy to see that, since X is connected, these Γ_i are conjugate to each other, and if $\Gamma' \subset \pi_1(U, b)$ is a subgroup conjugate to Γ_i, then $\Gamma' = \Gamma_j$ for some j. Therefore the intersection $\Gamma := \bigcap_{i=1}^{k} \Gamma_i$ is a normal subgroup of $\pi_1(U, b)$. Let (Y, b') be the quotient $\Gamma \backslash (\tilde{U}, \tilde{b})$. Then the natural projection $\tilde{p} : (Y, b') \to (U, b)$ is the Galois closure of each $(X, b_i) \to (U, b)$. The Galois group of $\tilde{p} : (Y, b') \to (U, b)$ is $\pi_1(U, b)/\Gamma$, which we shall denote by G. The image of the injection $\tilde{p}_* : \pi_1(Y, b') \to \pi_1(U, b)$ is just Γ. If we denote by $\alpha\langle Y, b'\rangle$ the lifting of α to Y such that $\alpha\langle Y, b'\rangle(0) = b'$, then

$$\Gamma = \{[\gamma] \in \pi_1(U, b) ; \gamma\langle Y, b'\rangle(1) = b'\} .$$

We denote by $H_i \subset G$ the group Γ_i/Γ. Then we see that these H_i are conjugate to each other, and for any $g \in G$ and i, $gH_ig^{-1} = H_j$ for some j. Moreover we have $\bigcap_{i=1}^{k} H_i = \{e\}$. This H_i is the Galois group of the Galois covering $(Y, b') \to (X, b_i)$, which we shall denote by $\tilde{q}_i$. This projection $\tilde{q}_i : (Y, b') \to (X, b_i)$ is given as follows.

We write $y \in Y$ as the endpoint of the lifting $\alpha\langle Y, b'\rangle$ of a path α on U such that $\alpha(0)=b$; $\alpha\langle Y, b'\rangle(1)=y$. Then by definition,

$$\tilde{q}_i(y)=\alpha\langle X, b_i\rangle(1) .$$

(Note that since $\Gamma \subset \Gamma_i$, the image $\tilde{q}_i(y)$ does not depend on the choice of α.)

Let us consider the relation between $\tilde{q}_i$ and $\tilde{q}_j$. Note that G acts on Y from left, because $\Gamma \subset \pi_1(U, b)$ acts on Y trivially as deck transformations. Let $[\gamma_{ij}] \in \pi_1(U, b)$ be an element such that $\gamma_{ij}\langle X, b_i\rangle = b_j$. Then we have $\Gamma_i = [\gamma_{ij}]\Gamma_j[\gamma_{ij}]^{-1}$. If $y=\alpha\langle Y, b'\rangle(1)$, then

$$\tilde{q}_j(y)=\alpha\langle X, b_j\rangle(1)=(\gamma_{ij}\alpha)\langle X, b_i\rangle(1) .$$

We put $g_{ij} := [\gamma_{ij}] \bmod \Gamma \in G$. Then, by the definition of the action of G on Y, we have

$$(\gamma_{ij}\alpha)\langle Y, b'\rangle(1)=g_{ij}(y) .$$

Therefore $\tilde{q}_j(y)=\tilde{q}_i(g_{ij}(y))$. Note that $\pi_1(U, b)$ acts on $B := p^{-1}(b)$ from right by

$$b_i^{[\gamma]}=\gamma\langle X, b_i\rangle(1) \qquad \text{for} \quad [\gamma] \in \pi_1(U, b) .$$

Since $\Gamma = \bigcap \Gamma_i$, $\Gamma \subset \pi_1(U, b)$ acts trivially on B. Hence G acts on B from right. Then $\gamma_{ij}\langle X, b_i\rangle = b_j$ is equivalent to $b_i^{g_{ij}} = b_j$. Combining these, we get

$$\tilde{q}_j=\tilde{q}_i \circ g_{ij} \qquad \text{where} \quad b_i^{g_{ij}}=b_j . \tag{1.1}$$

We have another way of describing Γ, Γ_i and G, H_i. We denote by $\mathfrak{S}(B)$ the permutation group of B, which acts from right on B. Let $\phi : \pi_1(U, b) \to \mathfrak{S}(B)$ be the natural homomorphism by the action defined above. Then we see that $\Gamma = \ker \phi$ and $G = \operatorname{im} \phi$. Since X is assumed to be connected, G acts on B transitively. Let $\mathfrak{S}(B, b_i) \subset \mathfrak{S}(B)$ be the stabilizer subgroup of $b_i \in B$. Then $\Gamma_i = \phi^{-1}(\mathfrak{S}(B, b_i))$ and $H_i = G \cap \mathfrak{S}(B, b_i)$. Note that G can be identified with $\tilde{p}^{-1}(b) \subset Y$ by

$$[\gamma] \bmod \Gamma \mapsto \gamma\langle Y, b'\rangle(1) . \tag{1.2}$$

Then the map $\tilde{p}^{-1}(b) \to B$ induced by $\tilde{q}_i$ is identified with the quotient map $G \to H_i \backslash G$. The image of $g \in G$ in $B \cong H_i \backslash G$ is given by b_i^g.

Now let C and D be the compactifications of X and Y, respectively. Then we have branched coverings $q_i : D \to C$ $(i=1, \cdots, k)$ extending $\tilde{q}_i$.

DEFINITION. We denote by $D_{ij} \subset C \times C$ the correspondence given by (q_i, q_j): $D \to C \times C$.

§ 2. Construction of the correspondences from the groups

We can start from the group G and the subgroup $H \subset G$.

Let G be a finite group and let $H \subset G$ be a subgroup such that

$$\bigcap_{g \in G} gHg^{-1}=\{e\} .$$

Then the action of G on $H\backslash G$ from right embeds G in the permutation group $\mathfrak{S}(H\backslash G)$ of $H\backslash G$. Let $U\subset\mathbb{P}^1$ be a non-empty Zariski open subset of $\mathbb{P}^1$, with a base point $b\in U$. Suppose that we are given a group homomorphism $\phi:\pi_1(U,b)\to\mathfrak{S}(H\backslash G)$ whose image coincides with G. From this ϕ, we can construct an étale covering $p:X\to U$ whose fiber $B:=p^{-1}(b)$ over b is canonically isomorphic to $H\backslash G$. This covering is the one given at the outset of the previous section. Let G act on G from right. Then, using ϕ, we get a homomorphism $\pi_1(U,b)\to\mathfrak{S}(G)$. The corresponding covering is the Galois closure $\tilde{p}:(Y,b')\to(U,b)$. Thus the fiber over b of $\tilde{p}$ is canonically isomorphic to G. We shall denote by $b_{Hg}\in B$ the point corresponding to $Hg\in H\backslash G$. Then we get morphisms $\tilde{q}_{Hg}:(Y,b')\to(X,b_{Hg})$ and $q_{Hg}:D\to C$.

DEFINITION. We denote by $D_{Hg,Hg'}\subset C\times C$ the correspondence given by $(q_{Hg},q_{Hg'}):D\to C\times C$.

§ 3. Endomorphisms on (co-)homology groups induced by the correspondences

We denote by $c_{ij}:H_1(C,\mathbb{Z})\to H_1(C,\mathbb{Z})$ and $c^{ij}:H^1(C,\mathbb{Z})\to H^1(C,\mathbb{Z})$ the endomorphisms of the homology and cohomology groups induced by the correspondence $D_{ij}\subset C\times C$.

The endomorphism c_{ij} is easy to describe. Let $\gamma\subset C$ be a 1-cycle representing $[\gamma]\in H_1(C,\mathbb{Z})$. Then $c_{ij}([\gamma])$ is represented by $q_j(q_i^{-1}(\gamma))$.

Now we shall describe $c^{ij}=q_{j*}\circ q_i^*$. Since G acts on D from left, we regard $H^1(D,\mathbb{C})$ as a right G-module. Let $h:H^1(D,\mathbb{C})\times H^1(D,\mathbb{C})\to\mathbb{C}$ be the non-degenerate bilinear form given by

$$h([\omega],[\eta]):=\int_D\omega\wedge\eta\,,$$

where ω and η are closed 1-forms on D representing the cohomology classes $[\omega]$ and $[\eta]$, respectively. Let $H^1(D,\mathbb{C})=V_i\oplus W_i$ be the decomposition such that V_i is the sum of all trivial H_i-submodules of $H^1(D,\mathbb{C})$ and W_i is the sum of all non-trivial irreducible H_i-submodules. Since the action of G preserves h, it is easy to see that V_i and W_i are orthogonal to each other with respect to h. Since $q_i:D\to C$ can be identified with the quotient morphism by H_i, the injection $q_i^*:H^1(C,\mathbb{C})\to H^1(D,\mathbb{C})$ identifies $H^1(C,\mathbb{C})$ with V_i. On the other hand, because the degree of $q_i:D\to C$ is $|H_i|$, the projection formula implies that the dual map $q_{i*}:H^1(D,\mathbb{C})\to H^1(C,\mathbb{C})$ of q_i^* is identified with $|H_i|$ times the natural projection $V_i\oplus W_i\to V_i$. Now suppose $b_j=b_i^{g_{ij}}$. Then we have $q_j=q_i\circ g_{ij}$ by (1.1). Since

$$\int_D\alpha^g\wedge\beta=\int_D\alpha\wedge\beta^{g^{-1}},$$

the dual action of g_{ij} on $H^1(D,\mathbb{C})$ with respect to h is given by g_{ij}^{-1}. Therefore $c^{ij}\otimes\mathbb{C}=q_{j*}\circ q_i^*=q_{i*}\circ g_{ij*}\circ q_i^*$ is given by

$$H^1(C, \mathbb{C}) \cong V_i \hookrightarrow V_i \oplus W_i \xrightarrow[g_{ij}^{-1}]{} V_i \oplus W_i \xrightarrow[|H_i| \cdot \mathrm{pr}_1]{} V_i \cong H^1(C, \mathbb{C}) .$$

The endomorphism $c_{\mathrm{hol}}^{ij} : H^1(C, \mathcal{O}) \to H^1(C, \mathcal{O})$ induced by $D_{ij} \subset C \times C$ can be described in the same way.

§ 4. The case when c_{ij} are multiplication by integers

PROPOSITION 1. *Suppose that G acts 2-transitively on B. Then c_{ij} $(i \neq j)$ is the multiplication by the integer $-|G|/(|B|^2 - |B|)$.*

Proof. Note that the natural homomorphism $\eta : \pi_1(X, b_k) \to H_1(C, \mathbb{Z})$ is surjective. We shall consider the image of $\eta([\gamma\langle X, b_k\rangle]) \in H_1(C, \mathbb{Z})$ via c_{ij}, where γ is the loop in U from b to b such that $[\gamma] \in \Gamma_k$, and $\gamma\langle X, b_k\rangle$ is the lifting of γ to X with the start point b_k. (Note that every element of $\pi_1(X, b_k)$ can be obtained in this way because of $\Gamma_k \cong \pi_1(X, b_k)$.) Since $H_1(C, \mathbb{Z})$ is torsion free and $\eta([\gamma^{|G|}\langle X, b_k\rangle]) = \eta([\gamma\langle X, b_k\rangle^{|G|}]) = |G| \cdot \eta([\gamma\langle X, b_k\rangle])$, it is enough to show that $c_{ij}(\eta([\gamma^{|G|}\langle X, b_k\rangle]) = (-|G|/(|B|^2 - |B|)) \cdot \eta([\gamma^{|G|}\langle X, b_k\rangle])$. Therefore we may assume that $[\gamma] \in \Gamma_k$ is contained in Γ. We identify $\tilde{p}^{-1}(b)$ with G by (1.2) and $B = p^{-1}(b)$ with $H_i \backslash G$. Recall that the image of $g \in G$ in $B \cong H_i \backslash G$ by q_i is given by b_i^g. Let $H_i g \in H_i \backslash G \cong B$ be the coset corresponding to b_k, (i.e., g is any element such that $b_i^g = b_k$.) Then $q_i^{-1}(\gamma\langle X, b_k\rangle)$ is the disjoint union of the loops $\gamma\langle Y, a\rangle$ where $a \in G \cong \tilde{p}^{-1}(b)$ runs through $H_i g \subset G$. (Note that since $[\gamma] \in \Gamma$, each $\gamma\langle Y, a\rangle$ is a loop.) Then $q_j(\gamma\langle Y, a\rangle) = \gamma\langle X, b_j^a\rangle$. Therefore

$$q_j(q_i^{-1}(\gamma\langle X, b_k\rangle)) = \sum_{a \in H_i g} \gamma\langle X, b_j^a\rangle ,$$

where the right hand side is the sum of 1-cycles (therefore with multiplicity). Since G acts 2-transitively on B, each element of $B \setminus \{b_k\}$ appears in $\{b_j^a ; a \in H_i g\}$ with multiplicity $|H_i|/(|B| - 1) = |G|/(|B|^2 - |B|)$, and b_k does not appear. On the other hand, since $H_1(\mathbb{P}^1, \mathbb{Z}) = 0$, we see that

$$\left[\coprod_{b_\nu \in B} \gamma\langle X, b_\nu\rangle\right] = \sum_{b_\nu \in B} [\gamma\langle X, b_\nu\rangle] = 0 \qquad \text{in} \quad H_1(C, \mathbb{Z}).$$

Therefore

$$[q_j(q_i^{-1}(\gamma\langle X, b_k\rangle))] = \frac{|G|}{(|B|^2 - |B|)} \sum_{b_\nu \in B \setminus \{b_k\}} [\gamma\langle X, b_\nu\rangle]$$

$$= -\frac{|G|}{(|B|^2 - |B|)} [\gamma\langle X, b_k\rangle] \qquad \text{in} \quad H_1(C, \mathbb{Z}) . \qquad \blacksquare$$

§ 5. Galois covering of algebraic curves and representations of the Galois group

In order to make use of the description of $c^{ij} \otimes \mathbb{C}$ and c^{ij}_{hol} in § 3, we have to know the representations of G on $H^1(D, \mathbb{C})$ and $H^1(D, \mathcal{O})$. In this section, we describe these actions in terms of the branching data $\phi : \pi_1(U, b) \to \mathfrak{S}(B)$. These can be done by the Lefschetz fixed point formula (cf. for example [3]) and the Hurwitz-Chevalley-Weil formula ([4], [1], see also [6]).

Let $\{P_1, \cdots, P_n\}$ be the complement $\mathbb{P}^1 \setminus U$. We fix a closed small disk Δ_i on $\mathbb{P}^1$ with the center P_i, and let $e_i \in \partial\Delta_i$ be a point on the boundary. Let ξ_i be the counter-clockwise loop from e_i to e_i along $\partial\Delta_i$, and let ω_i be a path in U from b to e_i. Let κ_i be the path $\omega_i \cdot \xi_i \cdot \omega_i^{-1}$. Then $[\kappa_i] \in \pi_1(U, b)$. We put $k_i := \phi([\kappa_i])$, and let $K_i \subset G$ be the cyclic subgroup generated by k_i.

Suppose that we are given a non-trivial irreducible representation ρ of G over $\mathbb{C}$ with the character χ. We put

$$\bar{\chi}\langle k_i \rangle = \sum_{\mu=0}^{|K_i|-1} \bar{\chi}(k_i^\mu),$$

$$\bar{\chi}_{\mathrm{hol}}\langle k_i \rangle = \frac{1}{2}\bar{\chi}(\mathrm{id}) + \sum_{\mu=1}^{|K_i|-1} \frac{\bar{\chi}(k_i^\mu)}{1-\zeta_i^\mu} \qquad \text{where} \quad \zeta_i = \exp\left(\frac{2\pi\sqrt{-1}}{|K_i|}\right).$$

Note that these depend only on the conjugacy class of k_i, and hence are independent of the choice of ω_i.

The following proposition can be proved easily by the (holomorphic) Lefschetz fixed point formula (cf. for example [3]). Combining this with the lemma below, whose proof is also easy, we get the classical Hurwitz-Chevalley-Weil formula.

PROPOSITION 2. *Let $m(\chi)$ and $m_{\mathrm{hol}}(\chi)$ be the multiplicities of the representation ρ in the G-modules $H^1(D, \mathbb{C})$ and $H^1(D, \mathcal{O})$ respectively. Then we have*

$$m(\chi) = -\sum_{i=1}^{n} \frac{\bar{\chi}\langle k_i \rangle}{|K_i|} + (n-2)\bar{\chi}(\mathrm{id}),$$

$$m_{\mathrm{hol}}(\chi) = -\sum_{i=1}^{n} \frac{\bar{\chi}_{\mathrm{hol}}\langle k_i \rangle}{|K_i|} + \frac{(n-2)}{2}\bar{\chi}(\mathrm{id}). \qquad \blacksquare$$

Let d be an integer ≥ 2, and $\zeta = \exp(2\pi\sqrt{-1}/d)$. For $v \in \mathbb{Z}/(d)$, we denote by $\langle\langle v \rangle\rangle$ the integer such that $v = \langle\langle v \rangle\rangle \bmod d$ and $1 \leq \langle\langle v \rangle\rangle \leq d$.

LEMMA. *We have*

$$\sum_{i=1}^{d-1} \frac{\zeta^{vi}}{1-\zeta^i} = \langle\langle v \rangle\rangle - \frac{d+1}{2}. \qquad \blacksquare$$

§ 6. Galois closure of the generic covering of $\mathbb{P}^1$

Let $f(X, Y)$ and $g(X, Y)$ be general homogeneous polynomials of degree d, and let $\Phi: \mathbb{P}^1 \to \mathbb{P}^1$ be the covering given by $(X: Y) \mapsto (f(X, Y): g(X, Y))$. Let $D_d \to \mathbb{P}^1$ be the Galois closure of Φ. It is obvious that, since f and g are general, the Galois group of $D_d \to \mathbb{P}^1$ is isomorphic to the full symmetric group $\mathfrak{S}_d$, and hence $\mathfrak{S}_d$ acts on D_d.

PROPOSITION 3. *Let χ be the character of a non-trivial irreducible representation ρ of $\mathfrak{S}_d$. Then the multiplicity $m(\chi)$ of ρ in the $\mathfrak{S}_d$-module $H^1(D_d, \mathbb{C})$ is given by*

$$m(\chi) = (d-3)\chi(\mathrm{id}) - (d-1)\chi(\text{transposition}) .$$

Proof. The number of the branch points of Φ is $2d-2$, and the ramification indexes of them are all 2. Therefore, each K_i $(i=1, \cdots, 2d-2)$ is a group of order 2 generated by a transposition. Since $\chi = \bar{\chi}$ for every character of $\mathfrak{S}_d$, we get the above formula from Proposition 2. ■

§ 7. Construction of algebraic curves C such that End(Jac(C)) contain the integer ring of a quadratic number field

Let $l = 2m+1$ be a prime number which is ≥ 5. We fix a generator s of $\mathbb{F}_l^\times$, and let t be s^2. Let G be the group

$$\langle \rho, \tau ; \rho^m = \tau^l = e, \tau\rho = \rho\tau^t \rangle .$$

(Since $\tau^l = e$, τ^t makes sense.) This group G can also be described as follows. Let $\tilde{\rho}$ and $\tilde{\tau}$ be generators of cyclic groups $\mathbb{Z}/(m)$ and $\mathbb{Z}/(l)$, respectively, which we shall denote multiplicatively. We let $\mathbb{Z}/(m)$ act on $\mathbb{Z}/(l)$ from left by $\tilde{\rho}(\tilde{\tau}) = \tilde{\tau}^{1/t}$. Then the semi-direct product of these cyclic groups by this action is isomorphic to G. Thus there is a natural surjective homomorphism $G \to \mathbb{Z}/(m)$ given by $\rho^a\tau^b \mapsto \rho^a$.

Let $H \subset G$ be the cyclic subgroup generated by ρ. Then H is not a normal subgroup, and

$$\bigcap_{g \in G} gHg^{-1} = \{e\}$$

holds. We fix an isomorphism of *sets*

$$H\backslash G \xrightarrow{\sim} \mathbb{Z}/(l)$$
$$H\tau^\mu \longmapsto \tilde{\tau}^\mu .$$

Then the action of G on $H\backslash G$ from right is given by

$$x^\tau = x\tilde{\tau}, \qquad \text{and} \qquad x^\rho = x^t ,$$

where $x \in \mathbb{Z}/(l) = \langle \tilde{\tau} \rangle$. The group G can also be described as a subgroup of the permutation group $\mathfrak{S}(\mathbb{Z}/(l))$ generated by the above two actions, where we regard

$\mathbb{Z}/(l)$ as a set.

Let U be a non-empty Zariski open subset of $\mathbb{P}^1$ with a base point $b \in U$, and let $\phi : \pi_1(U, b) \to \mathfrak{S}(\mathbb{Z}/(l))$ be a homomorphism such that the image of ϕ coincides with G. As above, let $X \to U$ be an étale covering of degree l corresponding to ϕ and let C be the compactification of X. Now we consider the endomorphism of the cohomology group $c_{\mathrm{hol}} : H^1(C, \mathcal{O}) \to H^1(C, \mathcal{O})$ induced by the correspondence $D_{H, H\tau^{-1}} \subset C \times C$.

We put $l^* = (-1)^{(l-1)/2} l$.

PROPOSITION 4. *There is a decomposition $H^1(C, \mathcal{O}) = H_+ \oplus H_-$ such that c_{hol} acts on H_+ (resp. H_-) as multiplication by $(-1+\sqrt{l^*})/2$ (resp. $(-1-\sqrt{l^*})/2$). Moreover if $l^* > 0$, then $\dim H_+ = \dim H_-$, while if $l^* < 0$, then $\dim H_+ - \dim H_-$ is divisible by the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{l^*})$.*

Proof. It is easy to check that all irreducible representations of G over $\mathbb{C}$ are given as follows; besides the trivial representation, G has $m-1$ one-dimensional representations which factor through the natural surjective homomorphism $G \to \mathbb{Z}/(m)$, and two m-dimensional irreducible representations ψ_+ and ψ_- which are given by

$$\psi_+(\tau) = \begin{pmatrix} \zeta & & & \\ & \zeta^t & & \\ & & \ddots & \\ & & & \zeta^{t^{m-1}} \end{pmatrix} \qquad \psi_+(\rho) = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ & & & 0 \\ & I_{m-1} & & \vdots \\ & & & 0 \end{pmatrix}$$

and

$$\psi_-(\tau) = \begin{pmatrix} \zeta^s & & & \\ & \zeta^{st} & & \\ & & \ddots & \\ & & & \zeta^{st^{m-1}} \end{pmatrix} \qquad \psi_-(\rho) = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ & & & 0 \\ & I_{m-1} & & \vdots \\ & & & 0 \end{pmatrix}$$

where $\zeta = \exp(2\pi\sqrt{-1}/l)$.

For an irreducible G-module M over $\mathbb{C}$, let $M = M' \oplus M''$ be the decomposition where M' is the sum of all trivial H-submodules and M'' is the sum of all non-trivial irreducible H-submodules. We denote by $c(M) \in \mathrm{End}(M')$ the composition

$$M' \hookrightarrow M \xrightarrow{\tau} M \xrightarrow{m \cdot \mathrm{pr}_1} M' .$$

If L is a non-trivial irreducible G-module of dimension 1, then $L' = 0$ and hence $c(L) = 0$. Let M_+ and M_- be the irreducible G-modules corresponding to ψ_+ and ψ_-, respectively. Then $\dim(M'_+) = \dim(M'_-) = 1$. Using the formula

$$\zeta^r+\zeta^{rt}+\cdots+\zeta^{rt^{m-1}}=\frac{1}{2}\left(-1+\left(\frac{r}{l}\right)\sqrt{l^*}\right)$$

for $r\in\mathbb{F}_l^\times$, we see that $c(M_+)$ and $c(M_-)$ are multiplications by $(-1+\sqrt{l^*})/2$ and $(-1-\sqrt{l^*})/2$, respectively.

Let D be the normalization of $D_{H,H\tau^{-1}}$, and let $H^1(D,\mathcal{O})=\bigoplus M_i$ be the decomposition of $H^1(D,\mathcal{O})$ into irreducible G-submodules. Since the quotient $G\backslash D$ is $\mathbb{P}^1$, there are no trivial G-submodules among $\{M_i\}$. Since the quotient $H\backslash D$ is C, we have $H^1(C,\mathcal{O})=\bigoplus M_i'$, and by the result of the section 3, c_{hol} acts on M_i' by $c(M_i)\in\mathrm{End}(M_i')$. Thus we get the desired decomposition $H^1(C,\mathcal{O})=H_+\oplus H_-$, and letting χ_+ and χ_- be the characters of ψ_+ and ψ_- respectively, we have proved that

$$\dim H_+=m_{\mathrm{hol}}(\chi_+)\qquad\text{and}\qquad\dim H_-=m_{\mathrm{hol}}(\chi_-)$$

where $m_{\mathrm{hol}}(\chi_\pm)$ are the multiplicities of $M_\pm$ among $\{M_i\}$.

Now we shall compute $m_{\mathrm{hol}}(\chi_+)-m_{\mathrm{hol}}(\chi_-)$. Let $K=\langle\rho^\alpha\tau^\beta\rangle\subset G$ be an arbitrary cyclic subgroup. Since

$$(\rho^\alpha\tau^\beta)^\nu=\rho^{\alpha\nu}\tau^{\beta(1+t^\alpha+\cdots+t^{\alpha(\nu-1)})},$$

we see that $K\cap\langle\tau\rangle=\{e\}$ if $\alpha\neq0 \bmod m$. Since $\chi_+(\rho^\alpha\tau^\beta)=\chi_-(\rho^\alpha\tau^\beta)=0$ if $\alpha\neq0 \bmod m$, we have

$$\chi_{+,\mathrm{hol}}\langle\rho^\alpha\tau^\beta\rangle=\chi_{-,\mathrm{hol}}\langle\rho^\alpha\tau^\beta\rangle=\frac{1}{2}m\qquad\text{if}\quad\alpha\neq0 \bmod m\,.$$

Let us compute $\chi_{\pm,\mathrm{hol}}\langle\tau^\beta\rangle$, where $\tau^\beta\neq e$. Using Lemma in the section 5, we have

$$\bar\chi_{+,\mathrm{hol}}\langle\tau^\beta\rangle=\frac{m}{2}+\sum_{i=0}^{m-1}\left(\langle\!\langle-\beta t^i\rangle\!\rangle-\frac{l+1}{2}\right),$$

$$\bar\chi_{-,\mathrm{hol}}\langle\tau^\beta\rangle=\frac{m}{2}+\sum_{i=0}^{m-1}\left(\langle\!\langle-\beta s t^i\rangle\!\rangle-\frac{l+1}{2}\right).$$

We put $(\mathbb{F}_l^\times)^2:=\{x^2;x\in\mathbb{F}_l^\times\}$. By the well-known formula for the class number $h:=h_{\mathbb{Q}(\sqrt{l^*})}$ of the imaginary quadratic fields (cf. for example [7]), we have

$$\begin{aligned}\bar\chi_{+,\mathrm{hol}}\langle\tau^\beta\rangle-\bar\chi_{-,\mathrm{hol}}\langle\tau^\beta\rangle&=\pm\left(\sum_{x\in(\mathbb{F}_l^\times)^2}\langle\!\langle x\rangle\!\rangle-\sum_{x\in(\mathbb{F}_l^\times)\setminus(\mathbb{F}_l^\times)^2}\langle\!\langle x\rangle\!\rangle\right)\\&=\pm\sum_{t=1}^{l-1}\left(\frac{t}{l}\right)t=\begin{cases}\mp l\cdot h\,, & \text{if}\quad l^*<0\,;\\ 0\,, & \text{if}\quad l^*>0\,.\end{cases}\end{aligned}$$

By Proposition 2, this completes the proof. ■

REMARK. In [5], Mestre constructed a family of curves of genus g whose jacobian varieties have an endomorphism induced by a real multiplication by $2\cos(2\pi/(2g+1))$. We can construct such curves using the dihedral groups by our

method.

References

[1] CHEVALLEY, C. and WEIL, A.; Über das Verhalten der Integrale erster Gattung bei Automorphismen des Functionenkörpers, *Abhand. Math. Sem. Humburg*, **10** (1934), 358–361.

[2] CILIBERTO, C., VAN DER GEER, G. and TEIXIDOR I BIGAS, M.; On the number of parameters of curves whose Jacobians possess nontrivial endomorphisms, *J. Algebraic Geom.*, **1** (1992), 215–229.

[3] GRIFFITHS, P. and HARRIS, J.; Principles of algebraic geometry, John Wiley & Sons, New York, 1978.

[4] HURWITZ, A.; Über algebraische Gebilde mit eindeutigen Transformationen in sich, *Math. Ann.*, **41** (1893), 403–441. Reprinted in Mathematische Werke, I, Birkhäuser, Basel, 1932, 392–436.

[5] MESTRE, J.-F.; Courbes hyperelliptiques à multiplications réelles, *C.R. Acad. Sci. Paris*, **307**, Série I, p. 721–724, 1988.

[6] MORRISON, I. and PINKHAM, H.; Galois Weierstrass points and Hurwitz characters, *Ann. Math.*, **124** (1986), 591–625.

[7] ONO, T.; An introduction to algebraic number theory, Plenum Press, New York, 1990.

Department of Mathematics
Faculty of Science, Hokkaido University
Sapporo 060, Japan